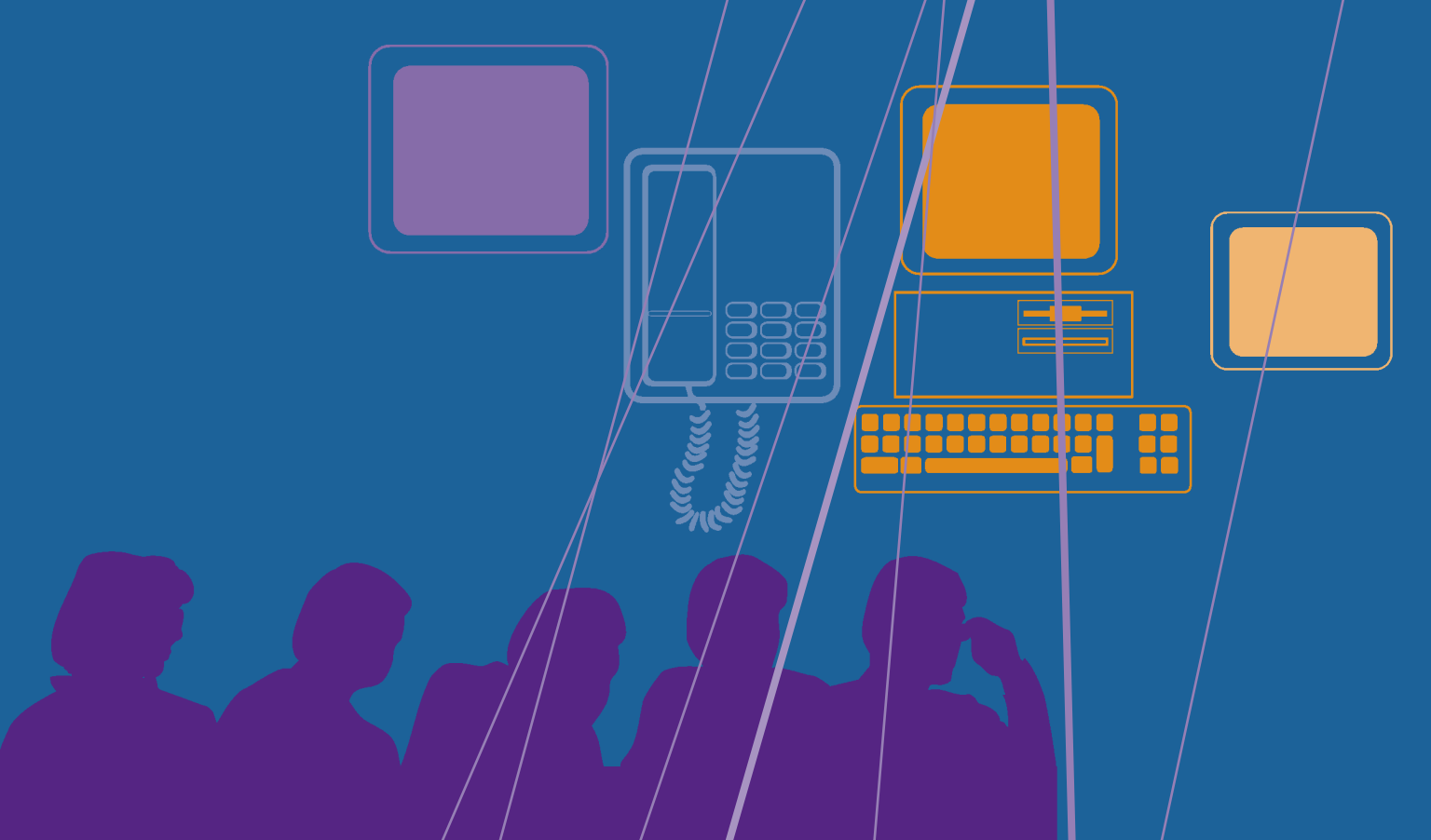




ELECTRONIC COMMUNICATIONS AT WORK

WHAT YOU NEED TO KNOW

ELECTRONIC COMMUNICATIONS AT WORK: What you need to know

Policy guidance produced by the Central Information Technology Unit, Cabinet Office

TABLE OF CONTENTS

1	OVERVIEW	1
	<i>An outline for senior managers of issues relating to the use and misuse of electronic communications.</i>	
	INTRODUCTION	1
	PURPOSE OF THIS GUIDANCE	1
	A POLICY STATEMENT OR CODE OF PRACTICE	1
	TRAINING STAFF IN USING ELECTRONIC COMMUNICATIONS	2
	AUDITING USAGE	2
2	THE POLICY STATEMENT OR CODE OF PRACTICE	3
	<i>Guidance for department and agency personnel units considering developing a policy statement or code of practice.</i>	
3	AUDITING, COMMUNICATIONS AND THE LAW	4
	<i>Information to help employers formulate a policy statement or code of practice.</i>	
	AUDITING EMPLOYEES' USE OF COMMUNICATIONS FACILITIES AT WORK	4
	Logging or baseline data audit	4
	Content audit	4
	GUIDANCE ON AUDITING	4
	REASONS TO AUDIT	5
	OTHER ISSUES TO CONSIDER	5
	AUDITING AND THE LAW	6
	The Data Protection Act 1984 and 1998	6
	European Convention on Human rights	6
	Human Rights Act 1998	6
	COMMUNICATIONS AND THE LAW	6
	Obscene Publications Act 1959	7
	Telecommunications Act 1984	7
	Protection of Children Act 1978; Criminal Justice Act 1988	7
	Protection from Harassment Act 1997; Sex Discrimination Act 1975; Race Relations Act 1976	7
	ILLEGAL CONTENT	7
	SERVICE PROVIDERS	7
	ANNEX A – AN EXAMPLE OF A COMPANY E-MAIL AND INTERNET POLICY	8
	ANNEX B – ABOUT THE INTERNET AND A GLOSSARY OF TERMS	10



Chapter 1 – Overview

An outline for senior managers of issues relating to the use of electronic communications.

Introduction

- 1.1** Fax machines, e-mail, voice mail, the Internet and video conferencing are widely used in today's workplace. They are powerful tools. Used properly, they can help organisations improve business performance. Staff can surf the Internet to research wide-ranging topics, all without leaving their desks; a fax machine or a PC can handle bulk distribution at the press of a couple of buttons.
- 1.2** The Government Secure Intranet (GSI) now gives departments a means of making the Internet accessible to all their staff. Many departments are connecting their internal networks and e-mail systems to the Internet via the GSI. However, browsing the World Wide Web and using external e-mail also raise significant management and legal issues.
- 1.3** The role of the Central Information Technology Unit (CITU) in the Cabinet Office is to advise Ministers on the development of their strategy for the use of information technology by Government. This strategy aims to ensure that the latest technology is harnessed to improve co-ordination across government and to improve the delivery of services to the public. As part of this work, CITU has produced this Guidance for departments and agencies to raise their awareness of the key issues involved for employers and employees in using electronic communications in the workplace.
- 1.4** With the use of electronic communications increasing, it is now a good time for employers to consider their policies on employees' use of these facilities. *CITU strongly recommends that departments and agencies issue such a policy statement or code of practice to all employees. In particular, they are strongly advised to draw up a management policy on auditing employees' e-mail and Internet usage.*

Purpose of this Guidance

- 1.5** The focus of this Guidance is to provide information on the issues related to the use of e-mails and the Internet. Chapter 1 clarifies for senior managers the problems that can arise concerning electronic communications in the workplace. Chapters 2 and 3 highlight the issues that department and agency personnel units might want to consider when drawing up communications policies and provide the information employers will need when formulating their policies and codes of practice.

A policy statement or code of practice

- 1.6** Departments and agencies may want to consider using this Guidance to draw up a combined communications policy that incorporates or refers to existing policies, for example on the use of telephones, IT security and equal opportunities and harassment. Concern about controlling unauthorised personal use of government-owned e-mail systems and the Internet is not a new problem – it just involves new technology. Departments and agencies will probably already have procedures to cover the misuse of other office resources, such as telephones, photocopiers or time. Misuse of e-mail or the Internet should be dealt with in the same way.

- 1.7** The possible scope of a code of practice is suggested in Chapter 2 – although departments and agencies will want to tailor it to their own management requirements. In essence, any policy or code of practice on the use of e-mails and the Internet should encourage reasonable, responsible and well-informed behaviour along with good management practice. Many organisations in both the public and private sector are beginning to put into place e-mail and Internet policies and an example of such a policy can be found at Annex A. For further examples and more information, the Internet provides a useful resource for finding out what other organisations are doing and the issues they have had to address. Two such sites are:
- <http://www.hobsonaudley.co.uk/mail.htm> (Hobson Audley Hopkins & Wood, a London law firm); and
 - <http://www2.echo.lu/legal/en/internet/content/communic.html> (Communication to the European Parliament).

Training staff in using electronic communications

- 1.8** Far from recommending a restrictive approach, CITU believes staff should be positively encouraged to become familiar with the Internet, e-mail and other facilities at their disposal. Many departments already promote this attitude, which will ensure that employees become confident, skilled users who are an asset to their organisation.
- 1.9** Departments and agencies will want to consider how they can help their staff to use new technology, such as e-mail and the Internet, effectively and efficiently. They will also need to consider how they can bring their departmental policy statement or code of practice to the attention of all employees. IT staff or contractors involved in auditing Internet use must be able to implement the policy or code of practice and have an understanding of the legal, auditing and privacy issues.
- 1.10** Formal training may be one way of developing the skills of staff. However, there are also informal, hands-on approaches that work just as effectively. The Department of the Environment, Transport and the Regions (DETR) is establishing an 'Internet café' facility, provided by its Library and Information Services branch, to support users who are new to the World Wide Web. The DETR has also issued a 'Golden Rules' note to employees on good practice in using e-mail.

Auditing usage

- 1.11** All organisations should tell staff clearly whether or not their use of the Internet and e-mail is being audited (i.e. logged, recorded and inspected). They should clearly define the circumstances in which the content of messages, as opposed to descriptive data, would be inspected. Staff should also be told what action will be taken if they breach management policy.
- 1.12** However, the decision on whether to audit and what to audit needs to take into account a number of issues. Chapter 3 provides further information.

Chapter 2

- The Policy Statement or Code of Practice

Guidance for department and agency personnel units considering developing a policy statement or code of practice.

2.1 Departments and agencies might wish to consider how best to:

- bring the policy or code to the attention of all staff when they join, and regularly after that;
- explain that communications facilities at work are there for the business purposes of the employer;
- ensure that employees know they are expected to behave responsibly when using communications facilities at work;
- reinforce the message that the department owns not only equipment and material, but also e-mails and downloaded Web pages;
- make clear that civil servants neither own the documents that they or their colleagues create, nor have intellectual property rights therein;
- provide guidelines if personal use is permitted;
- differentiate, where necessary, between media;
- explain what the audit process involves and inform employees of the consequences of any adverse audit;
- avoid *routine* content auditing;
- avoid *targeted* content auditing unless there is good reason to believe that the employee's usage contravenes criminal law, his/her employment contract, the Civil Service Code, discrimination law or amounts to a civil wrong (such as defamation);
- let employees see any personal electronic data collected through auditing and give them the right to dispute or amend inaccurate information;
- make it clear that a breach of policy could lead to disciplinary action and, in serious cases, termination of employment;
- advise employees on what to do if they encounter offensive material on the Internet accidentally;
- consult with relevant trade union representatives.

2.2 The code of practice could also refer to some possible infringements of policy, such as:

- creating, circulating, distributing, storing or downloading material that might be offensive, bring the department into disrepute or expose it to legal action. (Items deleted on PCs are recoverable and defamatory material can be restored and used as evidence against a department or individual.);
- using communications facilities at work for purposes that may be illegal, or contravene the Civil Service Code such as disclosing official information without proper authority;
- hacking, forging e-mail addresses, damaging government or other networks or using unlicensed software;
- bulk personal e-mailing (unless with permission);
- using communications facilities at work for unreasonably extensive private use (employees should be aware that all communications are considered to belong to the department and may be subject to auditing);
- sending particular categories of information electronically without security markings and/or encryption;
- not complying with the department's policy on electronic document management.

Information to help employers formulate a policy statement or code of practice.

Auditing employees' use of communications facilities at work

- 3.1 Departments and agencies need to consider whether there is a business need to audit the material their employees are sending and receiving or the Web sites they visit. The technical means of auditing services such as e-mail and access to the World Wide Web already exist. Some systems may already be gathering relevant information automatically – even if no one is looking at the resulting records. GSI security policy requires audit logs to be maintained on all traffic passing across the GSI. These are used for management of the network and to detect unauthorised activity such as hacking or security breaches by users of the GSI.
- 3.2 Auditing of e-mail and Web access falls into two main groups: 'logging', or the collection of baseline data, and the actual content of an e-mail. GSI does not routinely gather the content of e-mails.

Logging or baseline data audit

- 3.3 This type of audit provides a standard range of information. An Internet log would usually show the date, time, address of the computer using Internet Protocol (IP), address of the Web page (the Uniform Resource Locator or URL), type of command used (for example, File Transfer Protocol or FTP) and the name of any file accessed or downloaded. An e-mail log would contain details on the name of the sender, destination address or addresses, date and time sent and the size of the file.
- 3.4 The Data Protection Act 1998 does not stop departments or agencies using pre-announced routine or targeted audits, as long as they are either 'necessary for compliance with any legal obligation' or 'necessary for the purposes of legitimate interests pursued' (Schedule 2 of the Data Protection Act 1998). *Therefore, auditing would be acceptable if carried out as part of a published security policy, as long as users were advised in advance.*

Content audit

- 3.5 This form of audit looks inside the e-mail or Web page to see the actual contents. A department or agency is entitled to monitor the *content* of *work-related* e-mail and Internet usage for three main reasons: concern to reduce employer liability for employee action, manager's prerogative, and to prevent abuse of government-owned equipment.
- 3.6 The monitoring of the *content* of *personal* e-mail and Internet usage is a more involved issue. If an employee does not consent to the monitoring of personal e-mails then a department or agency runs the risk of contravening the Data Protection Act 1998 (once it is in force), breaching the implied duty of trust and respect and possibly infringing Article 8 of the European Convention on Human Rights (particularly once the Human Rights Act comes into force).

Guidance on auditing

- 3.7 The decision on whether to audit and what to audit is perhaps the most difficult issue when departments and agencies consider drawing up a policy statement or code of practice on e-mail and Internet usage. Although it is lawful to audit

employees' use of communications facilities at work, this is but one step in the process. Any audit policy needs to respect the right to privacy, comply with data protection law and observe the implied duty of trust between employer and employee. This suggests that routine or random auditing should be limited to 'logging' or collecting baseline data. Authorised staff operating a defined and documented auditing procedure should only access *content* in specified circumstances if they have good cause.

- 3.8** Any auditing procedures that are used should be transparent and employees should be aware of the process, purpose, and consequences of adverse findings, review mechanisms and right of access. Employees should also be given an indication of what data is being audited (baseline or content) and the system of auditing used, for example whether it is 'random', 'routine', 'targeted' or a combination of these.

Reasons to audit

- 3.9** Under UK law, employers are generally liable for what their employees do in the course of their work. This includes, for example, employees using e-mail or a fax machine to send defamatory messages.
- 3.10** Aside from liability issues, there are practical reasons why employers may wish to audit their employees' activities:
- Excessive personal use of e-mail and Internet services – as well as involving cost, this can affect the efficiency of the network system as a whole.
 - Security issues – sending protectively marked documents over unsecured telephone lines and networks and disclosing official information without proper authority. (Viruses can be imported from the Internet, too.)
 - Employees' behaviour in the way they use communications facilities at work could disrupt or damage the performance or reputation of the department.

Other issues to consider

- 3.11** If audit logs, or a similar system, are used to track Web sites or e-mail addresses used by employees, the resulting records, if they identify individuals, would amount to personal data for the purposes of the Data Protection Act 1998. The employee would be entitled to seek, and could expect to be given, access under Part II of that Act, unless one of the exceptions could be invoked. It is unlikely that third parties would be entitled to see the log.
- 3.12** If individuals bring their own laptops, palmtops or electronic diaries into the workplace and these items contain illegal or offensive material, then they should be treated in the same way as any other item brought into the workplace as covered by, for example, harassment or equal opportunity policies.
- 3.13** As there can be no possible legitimate business use for accessing or transmitting sexually explicit materials at work, the question of whether or not sexual material constitutes pornography is not relevant to the use of government-owned e-mail or Internet access.
- 3.14** Internet users can get connected accidentally to Web sites that contain illegal or offensive material. This can happen if users follow a link to a site whose content could not have been guessed at beforehand. Sometimes hyperlinks are hidden in Web sites and simply running the cursor over the link will take the user to another site which could contain illegal or offensive material. In this case, users could be advised to disconnect from the site immediately and inform either senior management or IT support.

- 3.15** As far as possible, contractors should be obliged by the terms and conditions of their contracts to follow the same principles and procedures as the department or agency which employs them. It is standard practice to ask contractors to observe confidentiality. Government departments and agencies will also have to comply with the seventh data protection principle of the Data Protection Act 1998 when it comes into force. This principle states:
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
- 3.16** The principle also obliges departments and agencies to choose contractors who can provide sufficient guarantees in these matters.
- 3.17** Contractors would be expected to abide by the same rules regarding the use of communications facilities as employees.

Auditing and the law

The Data Protection Act 1984 and 1998

- 3.18** Both the Data Protection Act 1984 and the Data Protection Act 1998 require departments and agencies to process computerised personal data 'fairly'. Auditing of e-mail or Internet usage will contravene the legislation unless it merely tracks overall patterns and does not allow identification of any particular employee's usage. Even if the data simply details Web sites visited by an individual or e-mail addresses, this would be enough to attract the statute. The 1998 Act does not prohibit pre-announced routine audits or targeted audits, but there must be a good reason: idle curiosity will not suffice, but concerns might cover expenditure, unlawful acts, suspicions about defamation, copyright infringement and harassment. Both the 1984 and the 1998 statutes in principle allow the employee access to any personal data collected by an audit.

European Convention on Human Rights

- 3.19** A public sector employee invoked the European Convention on Human Rights after her employer intercepted her telephone calls (*Halford v UK Government*). The European Court of Human Rights found that the secret interception of calls made by Ms Halford from her office amounted to an unjustifiable interference with her right to respect for her privacy and correspondence, contrary to Article 8(1) of the European Convention on Human Rights. A copy of the judgment is available on the Council of Europe's Web site (<http://www.dhdirhr.coe.fr>).

Human Rights Act 1998

- 3.20** The present Government's commitment to incorporating the European Convention on Human Rights into domestic law has led to the introduction of the Human Rights Act 1998. This Act will come into force in 2000. In future, a UK citizen would be able to assert their Convention rights through the national courts without having to take their cases to the European Court of Human Rights.

Communications and the law

- 3.21** There is a wide range of legislation available to tackle the potential criminal and civil liability issues that may arise from employees' misuse of communications facilities while at work. Some of the key statutes are briefly discussed below.
- If departments and agencies require specific information, they should seek legal advice.*

Obscene Publications Act 1959

- 3.22** All computer material is subject to the conditions of this Act, under which it is a criminal offence to publish an article whose effect, taken as a whole, would tend to deprave and corrupt those likely to read, see or hear it.
- 3.23** A computer disk, including the principal hard disk of the computer, can constitute an obscene article for the purposes of this Act if it contains or embodies matter that meets the test of obscenity. 'Publish' has a wide meaning and is defined as including distributing, circulating, selling, giving, lending, offering for sale or for lease. It seems clear that material posted to a newsgroup or published on a World Wide Web page falls within the legal definition of publishing and is therefore covered by the Act. The publisher would appear to be the originator or poster of the item.

Telecommunications Act 1984

- 3.24** The transmission of an obscene or indecent image from one computer to another via a 'public telecommunications system' is an offence under s.43 of this Act. For traditional mail, the same sort of offence is created under the Post Office Act 1953.

Protection of Children Act 1978; Criminal Justice Act 1988

- 3.25** These Acts make it a criminal offence to distribute or possess scanned, digital or computer-generated facsimile photographs of a child under 16 that are indecent.

Protection from Harassment Act 1997; Sex Discrimination Act 1975; Race Relations Act 1976

- 3.26** Harassment and discrimination are unlawful, whether or not the use of work-based communications facilities have played a role.

Illegal content

- 3.27** Illegal or unlawful content relates to a wide range of material that can be obtained from the Internet. The authors and providers of illegal material are held to be primarily responsible.

Service providers

- 3.28** Telecommunications and Internet service providers do not always offer adequate safeguards against illegal use. Many Internet service providers, such as Cable and Wireless, who provide GSI, are members of the Internet Service Providers' Association and the Internet Watch Foundation. As such, they agree to 'implement reasonable, practicable and proportionate measures to hinder the use of the Internet for illegal purposes, and to provide a response mechanism in cases where illegal material or activity is identified.' But this does not cover the full range of employers' issues and is mainly reactive; so it is still essential to have an independent, clear and comprehensive management policy.

Annex A

- An Example of a Company E-mail and Internet Policy

The following abridged version of an e-mail and Internet policy is reproduced with the kind permission of Field Fisher Waterhouse. The aim of including this paper is to provide a practical example of how one organisation has tackled this issue. A full version of the policy, which includes the full text for each of the six areas where legal issues might arise, can be obtained from: Richard Kenyon, Field Fisher Waterhouse, 35 Vine Street, London EC3N 2AA (e-mail rjk@ffwlaw.com).

INTRODUCTION

1. This Policy contains important rules covering e-mail and access to the Internet. Many of the rules apply equally to the Company's other methods of communicating with the outside world such as letter, fax and telephone.
2. This Policy explains how e-mail and Internet access should be used. It explains what you are allowed to do and what you are not allowed to do.
3. The Policy starts with some general rules covering dos and don'ts: We have then identified six areas where legal problems might arise for you and for the Company. These are harassment, defamation, copyright, entering contracts, pornography and confidential information. Under each section there is an explanation of the potential legal problems and some rules to help avoid those problems.
4. Failure to comply with the rules set out in this Policy:
 - a) may result in legal claims against you and the Company; and
 - b) may lead to disciplinary action being taken against you, including dismissal.
5. It is vital that you read this Policy carefully. If there is anything that you do not understand, it is your responsibility to ask your manager to explain. Once you have read and understood this Policy, you must sign it and then take a photocopy. Return the signed copy to the Human Resources Department and keep the photocopy for your own reference purposes.

GENERAL RULES: DOS AND DON'TS

1. The Company e-mail system is primarily for business use. Occasional and reasonable personal use is permitted provided that this does not interfere with the performance of your duties.
2. All e-mail is stored and the Company may inspect e-mail (including personal e-mail) at any time without notice.
3. If you send a personal e-mail, start or sign off the e-mail with the following statement:
Personal e-mail. This e-mail is personal. It is not authorised by or sent on behalf of the sender's employer. This e-mail is the personal responsibility of the sender.
4. Ask yourself, before sending an e-mail, how you would feel if your message was read out in Court. E-mail messages may have to be disclosed in litigation.
5. Obtain confirmation of receipt for important e-mails sent.
6. Make and keep hard copies of important e-mails sent and received.
7. Keep all passwords secure.
8. Check your e-mail on each working day or arrange for a duly authorised person to do so on your behalf.
9. Reply promptly to all e-mail messages requiring a reply. Where a prompt detailed response is not possible, send a short e-mail acknowledging receipt and giving an estimate of when a detailed response will/should be sent.
10. Do not impersonate any other person when using e-mail or amend messages received.
11. Do not import any non-text file, including files received as e-mail attachments, onto your system without first checking them for viruses, using the approved software.
12. Do not create e-mail congestion by sending trivial messages or personal messages or by copying e-mails to those who do not need to see them. Make use of the bulletin boards.
13. Do not access the World Wide Web for purposes other than those for which you are employed.
14. Do not deliberately visit, view, or download any material from any Web site containing sexual or illegal material or material which is offensive in any way whatsoever.
15. Do not subscribe to any bulletin boards, newsgroups or any other Internet service of any kind whatsoever without prior written permission from your manager.

16. Do not download software onto the company's system without the prior written permission of your manager. This includes software and shareware available for free on the Internet.

H A R A S S M E N T

What is harassment?

[Define term and refer to any existing organisational policy.]

What you must not do

[Provide examples of undesired behaviour/action.]

What are the consequences of not following this Policy?

[Explain any legal issues and refer to your organisation's disciplinary procedure.]

Reporting

[Explain your organisation's complaints procedure.]

D E F A M A T I O N

What is defamation?

[Define term and refer to any existing organisational policy.]

What you must not do

[Provide examples of undesired behaviour/action.]

What are the consequences of not following this policy?

[Explain any legal issues and refer to your organisation's disciplinary procedure.]

C O P Y R I G H T

What is copyright?

[Define term and refer to any existing organisational policy.]

What you must not do

[Provide examples of undesired behaviour/action.]

What are the consequences of not following this policy?

[Explain any legal issues and refer to your organisation's disciplinary procedure.]

E N T E R I N G C O N T R A C T S

What is a contract?

[Define term and refer to any existing organisational policy.]

Rules for contracting by e-mail

[Explain any existing organisational procedures/policies.]

What are the consequences of not following this policy?

[Explain any legal issues and refer to your organisation's disciplinary procedure.]

P O R N O G R A P H Y

What is pornography?

[Define term and refer to any existing organisational policy.]

What you must not do

[Provide examples of undesired behaviour/action.]

What are the consequences of not following this Policy?

[Explain any legal issues and refer to your organisation's disciplinary procedure.]

C O N F I D E N T I A L I N F O R M A T I O N

What is confidential information?

[Define term and refer to any existing organisational policy.]

What you must do and what you must not do

[Provide examples of undesired behaviour/action.]

What are the consequences of not following this Policy?

[Explain any legal issues and refer to your organisation's disciplinary procedure.]

A M E N D M E N T S

The Company may amend this Policy at any time.

What to do next

- 1. Sign and date the Policy
- 2. Photocopy the signed Policy.
- 3. Send the original Policy to Human Resources.
- 4. Keep the photocopy handy for reference purposes.

Signature

I have read through and understand the terms of this Policy.

Signature of Employee

.....

Date

.....

Annex B

- About the Internet and a Glossary of Terms

The term 'Internet' describes all the computers and networks around the world that 'talk' to each other. The world's telephone system – including satellites – is used as the infrastructure for the Internet.

Used properly, the Internet is a powerful tool for organisations. Its many benefits include worldwide communications, the sharing of resources and ideas, and access to a vast collection of resources. One of the key features of the Internet is that information from a single source can be viewed around the world. Even more important, no one country, group of companies or government can control the Internet or its content. It is estimated that around 60 million people currently use the Internet and the figure is doubling every year.

GLOSSARY OF TERMS

File Transfer Protocol (FTP)

The computer communications language used to move copies of files.

Hyperlink

Clicking on a hyperlink takes the user to a linked page (usually referred to as 'the link') which can be on any site anywhere on the World Wide Web. Hyperlinks often appear on Web pages as key words which are underlined.

HyperText Transfer Protocol (HTTP)

The most common method used to transfer information across the Web and to present it to the user when it arrives. The letters 'http' form part of most Uniform Resource Locators (URLs) used on the World Wide Web.

Internet Protocol (IP)

The mechanism for controlling the data which flow across the Internet.

IP address

The IP address is a unique identifier that can be used to locate the computer that sent a particular e-mail or visited a Web site.

Internet provider

Any organisation that offers a 'gateway' to the Internet. There are different types of provider:

- Internet access providers, specialising in offering access to the Internet;
- Internet service providers, offering access to the Internet and other services, such as hosting content produced either by users, third parties or themselves; and
- On-line service providers, offering Internet access and providing proprietary content for subscribers on their closed systems.

URL

Each Web page has an address called a Uniform Resource Locator which usually starts with 'http://www.' For example, the URL for the Central IT Unit at the Cabinet Office is 'http://www.citu.gov.uk'.

Web browser

A Web browser is the software that enables the user to access information on the Web. The two best-known are Microsoft Internet Explorer and Netscape Navigator.

Browsing and surfing

The words used to describe the activities of users as they follow leads and collect information.

Web page

The unit of information accessed by the user. Groups of pages linked together are referred to as a Web site.

Web server

A computer which hosts one or many Web sites and is permanently connected to the Internet. Special software is needed to run a Web server.

World Wide Web (WWW)

WWW, or 'Web' for short, is the collection of networks which make up the Internet.

ISBN 0 7115 0371 0

Central Information Technology Unit
Cabinet Office
53 Parliament Street
London SW1A 2NG
Telephone: 0171 238 2053
Facsimile: 0171 238 2081
E-mail: citu@citu.gov.uk

An electronic copy of this document is available at <http://www.citu.gov.uk>